WHAT IS CLAIMED IS:

1. A fingerprint authentication method comprising:

a first step of collating features of input data based on a fingerprint input by an user with features of enrolled data;

a second step of judging whether the input data are proper for authentication or not; and

a third step of authenticating the input data according to results of said first step and said second step; wherein

said second step is done on the basis of a spatial distribution of brightness in an input image represented by the input data.

2. A fingerprint authentication method as claimed in Claim 1, wherein said second step comprises:

a forth step of deciding a observation line on the input image;

a fifth step of finding a pair of peak envelopes each of which links local maximums or local minimums on a graph of brightness against positions on the observation line;

a sixth step of calculating discriminative values on the basis of the peak envelopes, said discriminative values representing features of the spatial distribution of the brightness; and

a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

3. A fingerprint authentication method as claimed in Claim 2, wherein said seventh step is done by the use of one or more discriminants and corresponding discriminative coefficients which are previously calculated.

4. A fingerprint authentication method as claimed in Claim 2, wherein said forth step comprises:

an eighth step of finding a fingerprint center and a fingertip direction on the input image; and

a ninth step of assuming two imaginary lines on the input image, one of said imaginary lines being parallel to the fingertip direction and used as the observation line, the other of said imaginary lines being perpendicular to the fingertip direction and used for another observation line.

5. A fingerprint authentication method as claimed in Claim 2, wherein said fifth step is done on the condition that distance between adjacent local maximums or adjacent local minimums is larger than a predetermined distance.

6. A fingerprint authentication method as claimed in Claim 5, wherein said predetermined distance is corresponding to an average ridge interval of a large number of samples.

7. A fingerprint authentication method as claimed in Claim 5, wherein said predetermined distance is corresponding to an average ridge interval calculated by applying Fourier transformation to a plurality of areas of the input image.

8. A fingerprint authentication method as claimed in Claim 2, wherein said sixth step is done on the basis of a spatial distribution function representing brightness against positions on the observation line, peak envelope functions representing said peak envelopes.

9. A fingerprint authentication method as claimed in Claim 2, further comprising:

a tenth step of requesting the user to input the fingerprint once more when decision that the input data are not proper is made at said seventh step.

10. A computer readable program for making a computer system serve as a finger authentication device, comprising:

a first step of collating features of input data based on a fingerprint input by an user with features of enrolled data;

a second step of judging whether the input data are proper for authentication or not; and

a third step of authenticating the input data according to results of said first step and said second step; wherein

said second step is done on the basis of a spatial distribution of brightness in an input image represented by the input data.

11. A computer readable program as claimed in Claim 10, wherein said second step comprises:

a forth step of deciding a observation line on the input image;

a fifth step of finding a pair of peak envelopes each of which links local maximums or local minimums on a graph of brightness against positions on the observation line;

a sixth step of calculating discriminative values on the basis of the peak envelopes, said discriminative values representing features of the spatial distribution of the brightness; and

a seventh step of deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

12. A computer readable program as claimed in Claim 11, wherein said seventh step is done by the use of one or more discriminants and corresponding discriminative coefficients which are previously calculated.

13. A computer readable program as claimed in Claim 11, wherein said forth step comprises:

an eighth step of finding a fingerprint center and a fingertip direction on the input image; and

a ninth step of assuming two imaginary lines on the input image, one of said imaginary lines being parallel to the fingertip direction and used as the observation line, the other of said imaginary lines being perpendicular to the fingertip direction and used for another observation line.

14. A computer readable program as claimed in Claim 11, wherein said fifth step is done on the condition that distance between adjacent local maximums or adjacent local minimums is larger than a predetermined distance.

15. A computer readable program as claimed in Claim 14, wherein said predetermined distance is corresponding to an average ridge interval of a large number of samples.

16. A computer readable program as claimed in Claim 14, wherein said predetermined distance is corresponding to an average ridge interval calculated by applying Fourier transformation to a plurality of areas of the input image.

17. A computer readable program as claimed in Claim 11, wherein said sixth step is done on the basis of a spatial distribution function representing brightness against positions on the observation line, peak envelope functions representing said peak envelopes.

18. A computer readable program as claimed in Claim 11, further comprising:

a tenth step of requesting the user to input the fingerprint once more when decision that the input data are not proper is made at said seventh step.

19. A fingerprint authentication device comprising:

a collating portion for collating features of input data based on a fingerprint input by an user with features of enrolled data;

a characteristic judging portion for judging whether the input data are proper for authentication or not; and

a authenticating portion for authenticating the input data according to outputs from said collation portion and said characteristic judging portion; wherein

said characteristic judging portion uses a spatial distribution of brightness in an input image represented by the input data to judge whether the

input data are proper for authentication or not.

20. A fingerprint authentication device as claimed in Claim 19, wherein said characteristic judging portion comprises:

an observation line deciding portion for deciding a observation line on the input image;

a peak envelope calculating portion for finding a pair of peak envelopes each of which links local maximums or local minimums on a graph of brightness against positions on the observation line;

a discriminative value calculating portion for calculating discriminative values on the basis of the peak envelopes, said discriminative values representing features of the spatial distribution of the brightness; and

a deciding portion for deciding whether the input data are proper for the authentication or not on the basis of the discriminative values.

21. A fingerprint authentication device as claimed in Claim 20, further comprises a discriminative coefficient holding portion for holding one or more discriminants and corresponding discriminative coefficients which are previously calculated by the use of said discriminants, wherein

said deciding portion uses said discriminants and said discriminative coefficients together with the discriminative values to decide whether the input data are proper for the authentication or not.

22. A fingerprint authentication device as claimed in Claim 20, wherein said observation line deciding portion executes of the steps of:

finding a fingerprint center and a fingertip direction on the input image; and

assuming two imaginary lines on the input image, one of said imaginary lines being parallel to the fingertip direction and used as the observation line, the other of said imaginary lines being perpendicular to the fingertip direction and used for another observation line.

23. A fingerprint authentication device as claimed in Claim 20, wherein said peak envelope calculating portion adopts a condition that distance between adjacent local maximums or adjacent local minimums is larger than a predetermined distance.

24. A fingerprint authentication device as claimed in Claim 23, wherein said predetermined distance is corresponding to an average ridge interval of a large number of samples.

25. A fingerprint authentication device as claimed in Claim 23, wherein said predetermined distance is corresponding to an average ridge interval calculated by applying Fourier transformation to a plurality of areas of the input image.

26. A fingerprint authentication device as claimed in Claim 20, wherein a discriminative value calculating portion calculates the discriminative values by the use of a spatial distribution function representing brightness against positions on the observation line, peak envelope functions representing said peak envelopes.

27. A fingerprint authentication device as claimed in Claim 20, wherein said authenticating portion requests the user to input the fingerprint once more when the input data are not proper.